AuCPace: Efficient verifier-based PAKE protocol tailored for the IIoT

Björn Haase and Benoît Labrique

Endress+Hauser Conducta GmbH&Co. KG, Germany
bjoern.haase@endress.com

Abstract.
Increasingly connectivity becomes integrated in products and devices that previously operated in a stand-alone setting. This observation holds for many consumer applications in the so-called "Internet of Things" (IoT) as well as for corresponding industry applications (IIoT), such as industrial process sensors. Often the only practicable means for authentication of human users is a password. The security of password-based authentication schemes frequently forms the weakest point of the security infrastructure.

Missing integration of IoT or IIoT device in a WEB-PKI should be considered a significant real-world risk. In this setting, verifier-based password-authenticated key-exchange (V-PAKE) protocols are known to provide a significant security improvement by preventing phishing and offline dictionary attacks.

For IIoT, availability concerns for the case of failures of (part of) the communication infrastructure makes local storage of access credentials mandatory. The larger threat of physical attacks makes it important to use memory-hard password hashing.

This paper presents a corresponding tailored protocol, AuCPace, together with a security proof within the Universal Composability (UC) framework considering fully adaptive adversaries. AuCPace uses CPace as a building block which could be used as a stand-alone balanced PAKE protocol. Moreover, we show how AuCPace could optionally provide for pre-computation attack resistance. In this paper we also introduce a new security notion of partially augmented PAKE that provides specific performance advantages for constrained servers.

We also present an actual instantiation of our protocol, AuCPace25519, and present performance results on ARM Cortex-M0 and Cortex-M4 microcontrollers, demonstrating the suitability of AuCPace for the constrained server setting.

This specific paper revision is an update of the journal version. It was setup for the PAKE selection process of the CFRG working group of the IETF for which AuCPace and CPace have been nominated.

Keywords: Password Authenticated Key Exchange, V-PAKE , PAKE, elliptic curves, Cryptographic Protocols, Universal Composability, IEC-62443, Industrial Control, Curve25519, X25519, OPRF

1 Introduction

Since recently, wireless and networking technology becomes integrated in products and devices that previously operated in a stand-alone setting, both in consumer applications in the so-called "Internet of Things" (IoT) as well as in the corresponding industry setting, the "Industrial IoT" (IIoT). Often communication technology and security protocols are employed that were not originally tailored and designed for the resource-constrained setting and the specific threat model.